INDEPENDENT EVALUATION PURSUANT TO THE GOVERNMENT INFORMATION SECURITY REFORM ACT FISCAL YEAR 2001

SENSITIVE BUT UNCLASSIFIED SYSTEMS

OFFICE OF THE INSPECTOR GENERAL EXECUTIVE SUMMARY

The Government Information Security Reform Act (GISRA) required the Office of the Inspector General (OIG) to perform an independent evaluation of the U.S. Department of Justice's (Department's) information security program and practices. This report summarizes the results of the evaluation for the Department's sensitive but unclassified (SBU) systems for FY 2001. Separate reports were issued for each of the individual systems evaluated. The OIG is also issuing a report summarizing the results of the Department's classified systems.

The OIG took an ambitious approach to fulfill the GISRA requirement by performing individual audits on a subset of Department systems. The OIG, in conjunction with Department management, selected four classified and five SBU systems to audit from the universe of Department systems for fiscal year 2001. Systems selected were mission critical and representative of differing system configurations (both client/server and mainframe) and operating systems (UNIX, Novell, Windows NT, and OS/390).

Under the direction of the OIG and in accordance with Government Auditing Standards, PricewaterhouseCoopers LLP conducted the assessment of the Department's overall computer security program and practices for the SBU systems by performing individual audits of five systems maintained by the Federal Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), Executive Office for U.S. Attorneys (EOUSA), and Justice Management Division (JMD).

SBU Systems Selected for Audit

Component	System
BOP	BOP Network (BOPNet)
DEA	El Paso Intelligence Center Information System (EIS)
DEA	Firebird
EOUSA	Justice Consolidated Office Network II (JCONII)
JMD	Rockville and Dallas Data Centers (JDC)

The audits consisted of interviews, on-site observations, and reviews of Department and component documentation to assess the system and component compliance with GISRA and related information security policies, procedures, standards, and guidelines. Commercial-off-the-shelf and proprietary software were used to conduct security tests and analyses of significant operating system integrity and security concerns.

The audits of the SBU systems revealed vulnerabilities with management (M), operational (O), and technical (T) controls. The auditors assessed these vulnerabilities at a high to low risk to the protection of each system and the data stored on it from unauthorized use, loss, or modification. Specifically, vulnerabilities were noted in the following areas:

Audit Results of SBU Systems

Areas of Vulnerability	Control Type	BOPNet	EIS	Firebird	JCONII	JDC
Security Policies and Procedures	M	✓	✓	✓	✓	✓
Authorization of Software Changes	M					✓
Risk Assessment Reporting	M	✓	✓	✓		
Contingency Planning	O		✓	✓		✓
System Backup Procedures	O			✓	✓	
System Configuration	O		✓	✓	✓	
Password Management	T	✓	✓	✓	✓	✓
Logon Management	T	✓	✓	✓	✓	✓
Account Integrity Management	T		✓	✓	✓	✓
System Auditing Management	T		✓	✓	✓	✓

Overall, the GISRA audits found that Department-level and component security policies and procedures were either insufficient or unenforced. The auditors concluded the Department did not provide timely and effective oversight to ensure implementation of its security policies. For example, the Department took nearly four years to revise its overall security policy, DOJ Order 2640.2D "Information Technology Security," after reporting it as ineffective in September 1997. In several areas of identified vulnerabilities, broadly stated or minimally imposed standards allowed system security managers too much latitude in establishing system settings, and consequently systems were not fully secured.

To address these deficiencies, we recommend granting responsibility to a single point of contact in the office of the Assistant Attorney General for Administration to oversee, standardize, implement, and maintain strict baseline Department-wide security controls over both SBU and classified systems. This contact also would serve as a liaison between the Information Management and Security Staff, the Security and Emergency Planning Staff, and the Assistant Attorney General for Administration. Among our recommendations are:

- enforce Department security policies at each component such as passwords, account lockout, and system auditing management;
- ensure that all components have current, documented, and tested contingency plans;
- develop a comprehensive corrective action plan to address weaknesses previously identified;
- ensure periodic computer security training is provided for each platform supported;
- ensure systems' security is monitored sufficiently, efficiently, and consistently, including:
  a) automated monitoring of security policy compliance and auditing of security relevant events;
  b) requiring intrusion detection testing and application and operating system patches be kept current.
- ensure that periodic updates supplement DOJ Order 2640.2D based on observed component needs, the evolving computer security environment, and industry best practices.

TABLE OF CONTENTS

INTRODUCTION

The fiscal year 2001 Defense Authorization Act (Public Law 106-398) includes Title X, subtitle G, "Government Information Security Reform Act" (GISRA). GISRA became effective on November 29, 2000, and amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." It requires federal agencies to:

- Have an annual independent evaluation of their information security program and practices performed.
- Ensure information security policy is founded on a continuous risk management cycle.
- Implement controls that assess information security risks.
- Promote continuing awareness of information security risks.
- Continually monitor and evaluate information security policy.
- Control effectiveness of information security practices.
- Provide a risk assessment and report on the security needs of the agencies' systems, and include the report in their budget request to the Office of Management and Budget (OMB).

In June 2001, the OMB issued "Reporting Instructions for the Government Information Security Reform Act," requiring the submission of an executive summary and a section characterizing the results of the OIG independent evaluation, by September 10, 2001.[1] The OIG coordinated GISRA work with the Department to promote communication and avoid duplication as the Department concurrently conducted program reviews to fulfill its GISRA obligations. The OIG also held briefings to keep Department and component management apprised of the audit results.

The OIG contracted with PricewaterhouseCoopers LLP to conduct the assessment of the overall computer security program and practices for the Department's sensitive but unclassified (SBU) systems. The objective was to determine the Department's compliance with the requirements of GISRA. To accomplish this objective, individual audits were performed on five SBU systems chosen by the OIG in consultation with Department management: the Drug Enforcement Administration's Firebird and El Paso Intelligence Center Information System, the Federal Bureau of Prisons Network, the Executive Office for U.S. Attorneys' Justice Consolidated Office Network II, and the Justice Management Division's Rockville and Dallas Data Centers.

[1] The OIG began the GISRA audits in April 2001, prior to the availability of OMB's GISRA reporting instructions. Therefore, our audits did not specifically address, and we do not report on, all of the instruction's 13 requested questions. However, we expect to include all 13 questions in the scope of our 2002 GISRA reviews.

The auditors reviewed management, operational, and technical controls by interviewing component management personnel, reviewing system documentation, and performing testing. The audits were performed in accordance with Government Auditing Standards and were conducted between April and August 2001. The audit approach was based on the General Accounting Office's Federal Information System Control Audit Manual, the Chief Information Officer Council Framework, and guidance established by the National Institute of Standards and Technology.

The OIG has routinely performed computer information security audits within Department components. Since 1996, the OIG also reviewed computer security program requirements annually as part of the financial statement audit process. For the GISRA audits, special emphasis was placed on reviewing vulnerabilities previously identified and verifying that appropriate corrective measures were implemented.

The GISRA audits of SBU systems revealed vulnerabilities with management, operational, and technical controls. The auditors assessed these vulnerabilities at a high to low risk to the protection of each system from unauthorized use, loss, or modification. Vulnerability assessments[2] were used to assess operational and technical controls of the SBU systems and identified serious deficiencies including weak password controls, inappropriate user privileges, improper intruder detection settings, and ineffective system auditing. Since technical controls prevent unauthorized access to system resources by restricting, controlling, and monitoring system access, we concluded that these vulnerabilities were the most significant.

The Department's Justice Management Division Information Management and Security Staff (IMSS) is responsible for providing guidance on security issues related to the Department's SBU systems. This includes monitoring components' compliance with the provisions of the Department's security policy and applicable Federal statutes, policies, and regulations as they apply to SBU computer systems. The IMSS has conducted network security penetration testing of SBU systems at Department components for the past four years.

A summary of the individual audit results previously reported is detailed in the Findings section of this report. Appendices I and II provide background on the systems selected and the objective, scope, and methodology for the audit.

[2] A vulnerability assessment is a security test in which evaluators analyze system settings and security features, based upon their understanding of the system design and implementation. A determination is then made as to whether the system is optimally configured and appropriate security controls are in place. Unlike penetration testing, vulnerability tests do not attempt to circumvent the security features of a system and gain entry.

FINDINGS

The Department's computer security program needs improvement to fully protect its SBU systems from unauthorized use, loss, or modification. Audits of five SBU systems disclosed vulnerabilities in management, operational, and technical controls as shown in the table below. Department-level and component security policies and procedures were insufficient or unenforced. The Department did not adequately: (1) identify and assess risks to determine needed security measures; (2) establish and implement policies and controls to meet those needs; (3) promote awareness so that users understand the risks and the related policies and controls required to mitigate them; or (4) monitor and evaluate established policies and controls to ensure that they were both appropriate and effective.

Control Type	BOPNet	EIS	Firebird	JCONII	JDC
MANAGEMENT CONTROLS	✓	✓	✓	✓	✓
OPERATIONAL CONTROLS		✓	✓	✓	✓
TECHNICAL CONTROLS	✓	✓	✓	✓	✓

I. MANAGEMENT CONTROLS

Management controls are techniques and concerns normally addressed by officials with responsibility for an organization's computer security program. In general, these controls manage the computer security program and the risk within the organization.

Security policies, procedures, standards, and guidelines are the primary means by which management communicates goals and requirements. To be effective, compliance must be overseen and enforced. The related policies should encompass all major systems and facilities. The policies should outline the duties of those who are responsible for overseeing security as well as the responsibility of those who own, use, or rely on the entity's computer resources.

The Department did not provide timely and effective oversight of SBU systems by informing users of the risks and the controls required to mitigate them or enforcing its own policies. Specifically, the audits disclosed vulnerabilities in the following areas:

Areas of Vulnerability	BOPNet	EPIC	Firebird	JCONII	JDC
Security Policies and Procedures	✓	✓	✓	✓	✓
Authorization of Software Changes					✓
Risk Assessment Reporting	✓	✓	✓		

Security Policies and Procedures

The Department established uniform policy, DOJ Order 2640.2C, "Telecommunications and Information System Security," dated June 25, 1993, for the protection of its automated information systems. Despite the rapid evolution of computer technology, this policy remained in effect and unchanged, governing the Department's information systems security environment for eight years. In a September 1997 audit, Report No. 97-26, "Computer Security at the Department of Justice," the OIG noted the Order's shortcomings and recommended that the Department develop effective computer security program guidance. However, the Department did not revise its policy, DOJ Order 2640.2D, "Information Technology Security," until four years later, in July 2001.

Although DOJ Order 2640.2D addresses many areas of identified system security vulnerabilities, the guidance remains insufficient for the protection of Department information systems. The Order imposes minimal standards that are broadly stated, allowing components and system security managers too much latitude in establishing system settings. To ensure uniform system security, DOJ Order 2640.2D needs more details in the following areas:

- backup procedures;
- access controls;
- assignment of user rights and advanced user rights;
- password management (including task versus user accounts);
- service accounts - changing the default password;
- logon management;
- renaming guest and administrative accounts;
- account integrity management, including monitoring of account disposition (dormant accounts); and
- accountability and audit trails.

Department-level guidance regarding the adequate, efficient, and consistent monitoring of SBU systems' security is also lacking. Specific areas that need addressing immediately are:

- automating the monitoring of security policy compliance;
- requiring timely software patch application;
- requiring intrusion detection testing; and

- automating the logging, auditing, review and notification of security relevant events.

Components are responsible for supplementing Department policy with more detailed written security policies, procedures, standards, and guidelines. Component and system level policies were also found to be inconsistently applied and ineffective. For all five systems audited, we found vulnerabilities attributed to inadequate security policies and ineffective enforcement. In addition, the OIG previously reported system security vulnerabilities attributable to unenforced and insufficient security policies on two systems that were not corrected.

Authorization of Software Changes

System software change management process provides for proper documentation and authorization of software changes, acceptance testing, management review and approval of changes and acceptance test results, and a controlled procedure for introducing tested and approved changes into production.

For the five systems reviewed, we found:

- One system's software change management process did not document approvals or installation and back-out plans.[3]

Risk Assessment Reporting

A risk is the possibility that a threat adversely impacts an information system by taking advantage of vulnerabilities. Thus, a risk assessment is a formal description and estimate of risk to an information system. After risks are identified, management should apply countermeasures relative to the severity of the threat and priority of asset protection.

For the five systems reviewed, we found:

- Two systems had vulnerabilities identified through risk assessments that were not corrected because appropriate management personnel never received the report or addressed its results.
- One system's risk assessment was outdated and did not reflect subsequent changes to the operating environment. As a result, management was unaware of potential system security exposures.

[3] Back-out plans are operator instructions for rolling-back new changes at implementation due to operational problems and restoring the previous software versions.

II. OPERATIONAL CONTROLS

Operational controls address security controls that are implemented and executed by people to improve the security of a particular system, often require technical or specialized expertise, and rely upon management activities as well as technical controls.

The auditors assessed the effectiveness of operational and technical controls by using commercial-off-the-shelf and proprietary software to conduct vulnerability assessments of the systems. A vulnerability assessment is a security test in which evaluators analyze system settings and security features based upon their understanding of the system design and implementation. A determination is then made as to whether the system is optimally configured and appropriate security controls are in place. Unlike penetration testing, vulnerability assessments do not attempt to circumvent the security features of a system and gain entry.

The audits identified vulnerabilities in the following areas:

Area of Vulnerability	BOPNet	EIS	Firebird	JCONII	JDC
Contingency Planning		✓	✓		✓
System Backup Procedures			✓	✓	
System Configuration		✓	✓	✓	

Contingency Planning

Effective contingency planning ensures continued operations by minimizing the risk of events that disrupt normal operations and by having an approach in place to respond to those events if they occur. Department policy requires that contingency plans be reviewed and approved by management.

Three of the five systems tested had one or more of the following vulnerabilities:

- Restoration priorities were not identified and an interagency agreement did not exist for the alternative processing site.
- Contingency plans were not properly reviewed or approved.
- Contingency plans were not tested.
- Contingency plan training was not conducted.
- The OIG previously reported a contingency planning vulnerability on one system that was not corrected.

System Backup Procedures

Backup procedures, including backup tapes, protect information resources, minimize the risk of unplanned interruptions, allow for recovery of critical operations when interruptions occur, and ensure on-going availability of critical system operations.

Industry best practices dictate that a backup storage location be off-site and far enough away from the primary location to avoid being impaired by the same events, such as fires, storms, and electrical power outages. Storing backup data tapes in the same location as the primary data risks completely losing all data in the event of a disaster.

For two of the five systems tested, we found:

- Backup tapes were not stored off-site, rendering backup data vulnerable in the event of a disaster at the primary location.

System Configuration

System configuration is the process of managing security features and assurances by regulating and monitoring changes made to hardware, software, firmware, and documentation throughout the lifecycle of an information system.

The Department's security policy requires that computer systems operate so that users have access to the information they need but no more and requires each computer system to have features or procedures to enforce access control measures required for the information in the system. Vulnerabilities with system configuration increase the risk that unauthorized users view, delete, or modify critical files, database intelligence data, or directory contents.

For three of the five systems audited, we found one or more of the following vulnerabilities:

- Network administrators were assigned inappropriate file permissions and user rights.
- Network File System (NFS) directories were mounted with inappropriate parameters, exported to users with read/write privileges, and exported to domains without fully qualified domain names.
- Highly vulnerable services were running on the networks.
- The latest manufacturer's patches were not installed.

- Versions of operating system software that are no longer supported by the vendor were used.
- Supporting software versions differed between development, test, and production environments.

The operational control vulnerabilities occurred due to a lack of Department and component guidance establishing and requiring appropriate system security standards and settings. Components did not adequately implement existing Department guidance, increasing the risk of unauthorized users obtaining access to system resources and exposing sensitive information to unauthorized use, loss, or modification.

III. TECHNICAL CONTROLS

Technical controls focus on the security controls that the computer system executes. Technical controls require significant operational considerations, should be consistent with the organization's security management, and depend upon the proper functioning of the system to be effective. Technical controls prevent unauthorized access to system resources by restricting, controlling, and monitoring system access and detecting and recording security related events.

The audits identified vulnerabilities with technical controls in the following areas:

Area of Vulnerability	BOPNet	EIS	Firebird	JCONII	JDC
Password Management	✓	✓	✓	✓	✓
Logon Management	✓	✓	✓	✓	✓
Account Integrity Management		✓	✓	✓	✓
System Auditing Management		✓	✓	✓	✓

Password Management

A password is a unique string of characters that must be provided before a logon or access is authorized to a computer system. Passwords are security measures used to restrict logons to user accounts and access to computer systems and resources. Strong password controls protect system resources from unauthorized use, loss, or modification.

All five systems tested had one or more of the following password management vulnerabilities:

- All five systems had inappropriate password recycle intervals, permitting users to re-use passwords too quickly.

- Four systems did not implement a "filter" enforcing password complexity rules.
- Four systems permitted users to have the same password for more than 90 days.
- Three systems either permitted blank or easily guessed passwords, such as a password equal to the user name.
- Three systems permitted user accounts with passwords less than eight characters.
- One system distributed user accounts using the Network Information System (NIS), exposing encrypted passwords to any user with the NIS password map.

Logon Management

The first line of defense against unauthorized access is an interactive logon process. The process normally begins with a warning banner, informing the user of the proper use of computers on the network. Next, the user is presented with a request for the user's information such as the username, password, and the server or domain the user intends to access. If the user's information is entered incorrectly, the system returns a logon failure message and, after a predetermined number of failed attempts, locks out the user for a specified period of time. If the user's information is entered correctly, the system authenticates the user, matching the user's information with an account in the system's security accounts database.

All five systems tested had one or more of the following logon management vulnerabilities:

- All five systems had inappropriate user or global systems settings, including the ability to make more than one simultaneous network connection; incorrect or disabled account login/lockout parameters; excessive grace logins; inappropriate screensaver settings; and settings that allow unauthenticated access and idle sessions.
- Four systems did not display a warning banner that informed users of the consequences of unauthorized access.
- Three systems did not follow their respective account naming conventions, impeding individual accountability for user activities.
- Three systems maintained inactive accounts, including accounts associated with terminated employees, accounts never used, or accounts without activity within the past ninety days.

- One system did not have the intruder detection option enabled, increasing the risk that unauthorized access would go undetected
- One system did not change vendor-supplied passwords upon software installation.

Account Integrity Management

Account integrity management controls the permissions for logging on to a computer or network. Proper expertise within a particular functional entity and clearly defined job duties and responsibilities are essential in maintaining a system. Monitoring resource access violations allows an entity to predefine a threshold for flagging violations. A privilege enables a user to perform a security relevant operation or a command that, by default, is normally denied to that user. Privileges must be tightly controlled and users clearly identified on the system in order to track their use of system resources.

Four of the five systems reviewed had one or more of the following account integrity management vulnerabilities:

- Four systems granted users inappropriate rights inconsistent with their duties.
- Three systems had inappropriate access to unrestricted shell accounts, allowing users access to unauthorized commands, data, and configuration files.
- Two systems allowed users to break out of their startup scripts giving users access to the command prompt.
- One system had systems programmers without appropriate training or oversight perform security administration duties.
- One system's security software global options were set inappropriately and generic logons were used to update critical systems software datasets without an independent technical review.
- One system had a root account trusting multiple servers through use of an ".rhosts" file that included one non-existent machine.
- One system did not use the Oracle product profile table and associated Oracle configuration utilities to implement appropriate security controls, allowing users to directly access and modify Oracle tables by circumventing application controls.

System Auditing Management

Auditing can provide the ability to detect and record security-related events. It tracks the activities of users by recording information about specific types of events, such as logon and logoff, file and object access, use of user rights, user and group management, security policy changes, restart, shutdown, and system events in a security log on the server.

For four of the five systems audited, we found one or more of the following system auditing management vulnerabilities:

- Three systems had auditing parameters incorrectly or inappropriately set such that critical events and modification to sensitive system applications, files, and registry keys could go undetected.
- One system's audit logs were not reviewed.
- One system was not set to secure event log files appropriately, increasing the risk of log file destruction or alteration.
- One system's programming activity was not monitored, increasing the likelihood that unauthorized and undetected changes to the system's environment may occur without appropriate review or oversight.

The technical control vulnerabilities occurred because Department policy was insufficient, not uniformly implemented, or not fully enforced. Further, the broadly stated, minimum standards imposed by the Department were not supplemented with sufficient or imposed component-level guidance to fully secure the systems. In several areas of identified vulnerabilities, broadly stated or minimally imposed standards allowed system security managers too much latitude in establishing system settings.

CONCLUSION

The GISRA audits of the SBU systems revealed vulnerabilities with management (M), operational (O), and technical (T) controls. The auditors assessed these vulnerabilities at a high to low risk to the protection of each system from unauthorized use, loss, or modification as shown in the table below.

Audit Results of SBU Systems

Areas of Vulnerability	Control Type	BOPNet	EIS	Firebird	JCONII	JDC
Security Policies and Procedures	M	✓	✓	✓	✓	✓
Authorization of Software Changes	M					✓
Risk Assessment Reporting	M	✓	✓	✓		
Contingency Planning	O		✓	✓		✓
System Backup Procedures	O			✓	✓	
System Configuration	O		✓	✓	✓	
Password Management	T	✓	✓	✓	✓	✓
Logon Management	T	✓	✓	✓	✓	✓
Account Integrity Management	T		✓	✓	✓	✓
System Auditing Management	T		✓	✓	✓	✓

Overall, the audits found that Department-level and component security policies and procedures were either insufficient or unenforced. The auditors concluded the Department did not provide timely and effective oversight to ensure implementation of its security policies. For example, the Department took nearly four years to revise its overall security policy, DOJ Order 2640.2D "Information Technology Security," after the OIG reported it as ineffective in September 1997. The Order imposes minimal standards that are broadly stated, allowing components and system security managers too much latitude in establishing system settings.

We recommend a proactive approach to improve security controls of Department systems. Because of the repetitive nature of the security deficiencies and concerns disclosed in this report, we conclude that a central office with responsibility for system security is needed to identify trends and enforce uniform standards. We believe that a central office would concentrate resources (time, money, and expertise) to identify and correct system security vulnerabilities most significant to the Department more effectively. Moreover, baseline security safeguards and controls should not vary according to the classification of system data, although data sensitivity might warrant additional or increased measures of protection.

In addition, senior management benefits from having a single point of contact responsible for overseeing activities that standardize, implement, and maintain strict, baseline Department-wide security controls over both types of systems. This office would also serve as a liaison between the Information Management and Security Staff, the Security and Emergency Planning Staff, and the Assistant Attorney General for Administration.

In the GISRA summary report for classified systems, the OIG made specific recommendations intended to improve Department-wide computer security for both the classified and SBU systems. These recommendations also apply to this report on SBU systems. We do not repeat these recommendations here, but for reference purposes, include them in Appendix III of this report.

APPENDIX I

BACKGROUND

PricewaterhouseCoopers LLP conducted the assessment of the overall computer security program and practices for the Department's sensitive but unclassified (SBU) systems by performing individual audits on five systems: the Federal Bureau of Prisons Network (BOPNet); the Drug Enforcement Administration's Firebird and El Paso Intelligence Center Information System (EIS); the Executive Office for U.S. Attorneys' Justice Consolidated Office Network II (JCONII); and the Justice Management Division's Rockville and Dallas Data Centers (JDCs).

The Federal Bureau of Prisons (BOP)

The mission of the BOP is to protect society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, and appropriately secure, and providing work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens. The BOP employs approximately 33,000 employees in its central office, six regional offices, and approximately 29 community correction management offices and 105 correctional facilities.

BOPNet

To fulfill its mission, the BOP uses automated information systems. One of its more critical information systems is the BOP Network (BOPNet). BOPNet is a SBU client/server-based network that interconnects the BOP central offices and nationwide facilities' workstations. BOPNet uses Novell Netware and Windows NT Server operating systems and provides users access to office automation software and BOP specific applications such as SENTRY. The BOP uses SENTRY to track its more than 158,300 prisoners.

The Drug Enforcement Administration (DEA)

The mission of the DEA is to enforce controlled substances laws and regulations of the United States and investigate organizations and individuals that grow, manufacture, or distribute controlled substances. The DEA also recommends and supports non-enforcement programs that are designed to reduce the availability of illicit controlled substances worldwide.

Firebird

Firebird is a SBU system that provides office automation tools, e-mail communications, on-line case file database access, and other information resources to DEA administrative, investigative, analytical, and technical support personnel. Because of the sensitive nature of the data processed on Firebird, a compromise of the system could jeopardize the confidentiality of investigations and agent safety. Firebird is a client/server-based system using Windows NT and UNIX operating systems.

EIS

The El Paso Intelligence Center (EPIC) is located on Biggs Army Airfield, an extension of Fort Bliss, in El Paso, Texas. Biggs Army Airfield is a controlled access United States Army military installation. Organizationally, EPIC is under the direct line authority of the DEA. EPIC management is comprised of senior law enforcement representatives from several states and 15 federal agencies. Overall coordination of EPIC activities is the responsibility of the EPIC Director. EPIC's mission is to support United States law enforcement and interdiction components through the timely analysis and dissemination of intelligence on illicit drug and alien movements and the criminal organizations responsible for these illegal activities.

The EPIC Information System (EIS) processes data types, ranging in classification from law enforcement sensitive to secret high[4], that encompass historical intelligence, tactical, administrative, and office automation data. The EIS is a mission critical operation that select EPIC personnel access 24 hours a day, seven-days a week, with classified and unclassified sections operating separately. This report summarizes the audit results of the unclassified EIS section.

The EIS was designed to collect, process, and disseminate intelligence information concerning the movement of illicit drugs and currency, alien smuggling, weapons trafficking, and other illegal related activities. The primary repository of the unclassified intelligence data is the EPIC Internal Database (EID). The EID is an Oracle database accessed through a combination of custom developed and commercial-off-the-shelf software. The EID stores suspect and tracking files on people, organizations, vehicles, vessels, aircraft, and associated events for all unclassified intelligence collected at EPIC.

[4] "Secret high" is a DEA sensitivity rating.

The Executive Office for U.S. Attorneys (EOUSA)

The mission of the EOUSA is to provide the 94 United States Attorney Offices located throughout the 50 states, the District of Columbia, Guam, the Marianas Islands, Puerto Rico, and the U.S. Virgin Islands with general executive assistance, operational and administrative support, and coordination with Department of Justice components and other federal agencies.

JCONII

The Justice Consolidated Office Network II (JCONII) is a SBU system designed to be the office automation system for the Department's management, litigating, and related legal components.

Administrative support is facilitated through the use of commercial-off-the-shelf applications residing on EOUSA's JCONII. United States Attorneys use JCONII to access legal applications and EOUSA proprietary software. The JCONII system is a client/server-based network using both Windows NT and UNIX platforms.

The Justice Management Division (JMD)

The JMD Information Management and Security Staff's (IMSS) mission is to be the principal point of coordination in DOJ for compliance with federal agency requirements under information technology (IT) laws and directives. IMSS develops and implements policies, procedures, and guidance for IT architecture and strategic planning, IT investment management, and the security of the Department's SBU information systems.

JDCs

The Department of Justice maintains legacy[5] systems housed on mainframe platforms at data centers in Rockville, Maryland and Dallas, Texas. The Rockville and Dallas data centers (JDCs) exist to provide secure information technology facilities, computing platforms, and support services for the bureaus, offices, boards, and divisions within the Department. Since the JDCs are managed as one unit, they were audited as a combined entity.

[5] "Legacy" refers to traditional electronic data processing general support systems and applications running on mainframe computers with programming and operational support maintained in a centralized information technology environment.

APPENDIX II

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audits was to determine the Department's compliance with the requirements of the Government Information Security Reform Act. In doing so, the OIG assessed whether adequate computer security controls existed to protect Department systems from unauthorized use, loss, or modification. To accomplish the objective, the OIG reviewed management, operational, and technical controls for a subset of Department systems. This report summarizes the audit results of the five SBU systems reviewed.

We interviewed component and system management personnel, reviewed system documentation, and performed testing to determine compliance with Department and component security policies and procedures. The audits were performed in accordance with Government Auditing Standards and took place from April through August 2001. The effectiveness of security controls was assessed by using commercial-off-the-shelf and proprietary software to conduct vulnerability assessments of the system.

The audit approach was based on the General Accounting Office's Federal Information System Controls Audit Manual, the Chief Information Officer Council Framework, OMB Circular A-130, and guidance established by the National Institute of Standards and Technology.

APPENDIX III

RECOMMENDATIONS[6]

We recommend that the Acting Assistant Attorney General for Administration (AAG/A):

1) Establish a Department Information Technology (IT) Central Security Compliance Office for classified and sensitive but unclassified systems with the responsibility for:

   a) Monitoring security-related activities by testing controls at each component having classified systems (i.e. performing penetration tests and providing those results to the affected components).

   b) Reviewing the number and types of security deficiencies identified in each component's periodic reports.

   c) Evaluating each component's compliance with Department security policies especially in areas of reported weaknesses and establishing processes and procedures to enforce existing policy such as passwords, account lockout, and system auditing management.

   d) Assisting component Security Program Managers in assessing security risks, identifying hardware/software security deficiencies, and providing policy and procedural guidance as needed.

2) Charge the Department IT Central Security Compliance Office with ensuring that all components have current, documented, and tested contingency plans.

3) Charge the Department IT Central Security Compliance Office with developing a comprehensive corrective action plan to fully and timely address all Department-wide IT control weaknesses previously identified in security reviews and audits. Additionally, measures should be prescribed and oversight provided to ensure that component corrective action plans are prepared and that vulnerabilities are corrected. Eliminating repeat findings should be a priority.

[6] These recommendations are presented in our GISRA summary report for classified systems. Corrective action will be tracked as part of the follow-up process for that report. See Appendix IV.

4) Require each component Security Program Manager to:

   a) Have full knowledge of and familiarization with current Department information technology security policies and procedures, including DOJ Order 2640.2D and other departmental policies related to classified and unclassified systems.

   b) Report component compliance with Department security policy requirements.

   c) Ensure a security administrator is designated within each component for reviewing system security posture in accordance with Department security policy. In the case of multiple platforms or operating systems supporting component systems, an administrator should be designated to represent each unique platform.

   d) Ensure periodic computer security training is provided for each platform supported and require attendance by the designated security administrators.

   e) Develop and enforce security policies or apply industry best practices, to assess and counter evolving computer security vulnerabilities.

5) Require each component Security Program Manager to periodically report to the Department IT Central Security Compliance Office on the compliance of individual systems within their component relative to requirements outlined in Department security policies and procedures. Upon its review of the reports, the Department IT Central Security Compliance Office should bring areas of concern to the attention of the AAG/A.

6) Establish and implement guidance to ensure systems' security is monitored sufficiently, efficiently, and consistently. Specific areas that need to be immediately addressed include:

   a) automated monitoring of security policy compliance;

   b) automated logging, auditing, review and notification of security relevant events;

   c) requiring intrusion detection testing; and

   d) requiring application and operating system patches be kept current.

   (Note: According to JMD, they began addressing some of the above areas after the audits were completed.)

Although DOJ Order 2640.2D addresses many areas of identified system security vulnerabilities, it still lacks sufficient guidance in several areas. The policy should be specific to each operating system (Windows NT, Novell, and UNIX) so that the requirements are not misunderstood or inappropriately applied (i.e. some procedures may apply to Windows NT systems but not to UNIX systems). Further, procedures need to be developed to provide more specific guidance when necessary.

Therefore, we recommend that the AAG/A:

7) Require periodic updates that supplement DOJ Order 2640.2D based on observed component needs, the evolving computer security environment, and industry best practices. We recommend that the AAG/A promptly review the adequacy of guidance for the following areas:

   a) password management (including task versus user accounts);

   b) accountability and audit trails;

   c) access controls;

   d) account integrity management, including monitoring of account disposition (dormant accounts);

   e) logon management;

   f) service accounts - changing the default password;

   g) assignment of user rights and advanced user rights;

   h) renaming guest and administrative accounts; and

   i) backup procedures.

APPENDIX IV

VIEWS OF RESPONSIBLE OFFICIALS AND STATUS OF REPORT

In the GISRA summary report for classified systems, the OIG made specific recommendations intended to improve Department-wide computer security. Although those recommendations are applicable to both the classified and SBU systems, they are included in this report for reference purposes only and will be tracked as part of the follow-up process of the GISRA summary report for classified systems.

We issued this report in draft to obtain review and comment from responsible Department officials. The Acting Assistant Attorney General and Chief Information Officer responded that they had no comments. There are no recommendations in this report. Therefore, this report is closed.